Claims:

What is claimed is:

1. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

f) encrypting the first electronic key using a first encryption key of the key provider;

g) providing within the second other system a first secure module having a second encryption key within a read-only memory circuit thereof and provided with the first secure module, the second encryption key accessible only by program code being executed on a processor internal to the first secure module, and wherein the second encryption key is other than modifiable and other than accessible outside of the module;

h) transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

i) providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

j) executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the read-only memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

2. The method according to claim 1 wherein the processor internal to the module accesses the second encryption key only for decrypting encrypted electronic keys, wherein the decrypted electronic keys are then stored within the module inaccessible outside the secure module.

3. The method according to claim 2 wherein the step (a) is performed in a corresponding secure module.

4. The method according to claim 3 wherein the processor internal to the module accesses the second encryption key only in response to a request from a corresponding secure module.

5. The method according to claim 4 wherein the second encryption key and the first encryption key are the private and public portions of an asymmetric private/public-key pair, respectively.

6. The method according to claim 4 wherein the second encryption key and the first encryption key are a same private key for use with a symmetric key-based encryption algorithm.

7. The method according to claim 6 comprising the additional step prior to step a) of:

a1) generating a first electronic key within a key-generating processor internal to the key provider system.

8. The method according to claim 7 wherein the key-generating processor is embodied on the corresponding secure module.

9. The method according to claim 6 wherein the first electronic key is a root key for use in at least one of encrypting and decrypting private encryption keys.

10. A method for transferring a first electronic key between a key provider system and a second other system via an information network comprising the steps of:

a) encrypting the first electronic key using a first encryption key of the key provider;

g) providing within the second other system a first secure module having second and third encryption keys within a memory circuit thereof, the second and third encryption keys accessible only by program code being executed on a processor internal to the first secure module for decrypting encrypted electronic keys and for storing the decrypted electronic keys within a memory circuit of the first secure module, and wherein the second and third encryption keys are other than accessible outside of the module;

h) transferring the encrypted first electronic key from the key provider system to the second other system via the information network;

i) providing the encrypted first electronic key to the processor internal to the first secure module of the second other system; and,

j) executing program code on the processor internal to the first secure module to decrypt the encrypted first electronic key using the second encryption key stored within the memory circuit of the first secure module and to store the decrypted first electronic key internally within a secure key memory location of the first secure module.

11. A method for transferring a first electronic key between a key provider system and a second other system via an information network according to claim 10 comprising the steps of:

k) encrypting a fourth encryption key using one of the third encryption key and a key corresponding to the third encryption key;

l) transferring the encrypted fourth encryption key from the key provider system to the second other system via the information network;

m) providing the encrypted fourth encryption key to the processor internal to the first secure module of the second other system; and,

n) executing program code on the processor internal to the first secure module to decrypt the encrypted fourth encryption key using the third encryption key stored within the memory circuit of the first secure module and to store the decrypted fourth encryption key within the memory circuit of the first secure module at a location corresponding approximately to the location where the second encryption key was stored.

12. The method according to claim 11 wherein the second and third encryption keys are only replaceable through use of another of the second and third encryption keys.

13. The method according to claim 12 wherein the second, third and fourth encryption keys are super-root keys for at least one of encrypting and decrypting root keys.

14. The method according to claim 11 wherein the step of storing the decrypted fourth encryption key comprises the steps of:

f1) erasing the second encryption key from a first storage area of the memory circuit; and,

f2) storing the decrypted fourth encryption key within approximately the same first storage area of the same memory circuit.

15. A system for transferring a secure electronic key between a key provider system and a second other system via an information network that is other than secure comprising a secure module in operative communication with the second other system, the secure module including:

an encryption processor;

an input port for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor;

a memory circuit in operative communication with the encryption processor for storing at least a first encryption key;

memory storage having program code stored therein and executable on the encryption processor for, upon receipt of an encrypted secure electronic key, decrypting the encrypted secure electronic key using the at least a first encryption key and for storing the decrypted secure electronic key within the memory circuit, the at least a first encryption key being other than accessible by any code other than the program code and being other than modifiable thereby.

16. The system according to claim 15 wherein the code executable on the encryption processor accesses the at least a first encryption key only in response to a request from a corresponding secure module.

17. The system according to claim 16 wherein the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

18. The system according to claim 17 wherein the memory circuit for storing the at least a first encryption key is a read-only memory circuit.

19. The system according to claim 18 wherein the module is FIPS 140 compliant.

20. The system according to claim 19 wherein the module includes a tamper detection circuit for erasing the first cryptographic key in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.

21. A system for transferring a secure electronic key between a key provider system and a second other system via an information network that is other than secure comprising a secure module in operative communication with the second other system, the secure module including:

an encryption processor;

an input port for receiving encrypted electronic data from outside the module and for providing the encrypted electronic data to the encryption processor;

a memory circuit in operative communication with the encryption processor for storing a first encryption key within a first memory location thereof and for storing a second encryption key within a second other memory location thereof;

memory storage having program code stored therein and executable on the encryption processor for, upon receipt of an encrypted third encryption key from the second other system, decrypting the encrypted third encryption key using one of the first and second encryption keys and for storing the decrypted third encryption key approximately within the same memory location of the other one of the first and second encryption keys, the first and second encryption keys being other than accessible by any code other than the program code and being other than modifiable absent erasing thereof by any code other than the program code.

22. The system according to claim 21 wherein the code executable on the encryption processor accesses the first and second encryption keys only in response to a request from a corresponding secure module.

23. The system according to claim 22 wherein the code executable on the encryption processor is only for performing encryption functions the results of which are inaccessible outside of the module.

24. The system according to claim 23 wherein the memory circuit for storing the first and second encryption keys is a substantially non-volatile reprogrammable memory circuit.

25. The system according to claim 24 wherein the substantially non-volatile reprogrammable memory circuit is one of an electrically erasable read-only memory (EEPROM) circuit and a random access memory (RAM) circuit having an on-board power supply in the form of a battery.

26. The system according to claim 25 wherein the module is FIPS 140 compliant.

27. The system according to claim 26 wherein the module includes a tamper detection circuit for erasing every cryptographic key stored within the memory circuit in dependence upon a detected attempt to access the electronic contents of the module in an unauthorized fashion.